Privacy risks when using mobile devices in health care

Matthew Bromwich MD, Rebecca Bromwich LLM PhD

Use of mobile devices has offered physicians new ways to conduct professional communication, easier access to decision support and expedited, efficient specialist consultation. However, risks associated with the use of smart phones to produce and store medical images include privacy breaches, insecure data storage and physician or institution liability for failure to obtain patient consent. Consumer mobile apps for photo documentation do not meet standards of care reasonably expected to ensure patient privacy and the secure storage of medical documentation. Two lawsuits currently proceeding through the Canadian courts address privacy breaches in health care.

The Supreme Court of Canada, in *McInerney* v. *MacDonald,* characterized individuals' medical records as private, sensitive and personal (Appendix 1, available at www.cmaj.ca/lookup/suppl/doi:10.1503/cmaj.160026/-/DC1). Many institutions now opt for a bring-your-own-device (BYOD) approach,[1] which limits options for implementing security measures. What are the risks when physicians use their own devices (e.g., to capture an image or video material) in the health care setting?

It might be considered that implicit patient consent could be fairly assumed when patient data, including traditionally acquired photos, are collected in the course of providing clinical care. However, explicit consent is required for the purposes of education, research and publication; therefore, it is advisable to obtain consent at the time of capture and store this consent with any images taken, especially when using a mobile platform that may pose special privacy concerns.

Potential for security breaches if electronic mobile devices are hacked, lost or stolen means that recording, storing and sharing patient information or images on such devices is risky.[2] Dropbox, iCloud, Facebook, Google Plus and Instagram are among an expanding group of apps programmed with the capability to automatically access documents and images stored on mobile devices. Images can be easily, even inadvertently, shared widely on social networks, or backed up on nonsecure systems. Data can become public quite easily without sufficient safeguards.

What are the standards for privacy? Provincial and territorial legislation across Canada governs the privacy of medical records. For example, according to the Medicine Act of Ontario, any materials, including photos, used for the purposes of clinical care or decision-making are considered part of the medical record. Similar laws apply in other provinces and territories. Patient data should be labelled, logged and secured. Failing to protect the privacy of medical records can lead to disciplinary, regulatory and criminal penalties. For example, breach in privacy of personal health information is defined in Ontario as an "impermissible use" or "disclosure" under the privacy rule that compromises the security or privacy of the protected health information.

Guidance from regulators and hospitals regarding mobile devices is evolving. Each of the Canadian Medical Protective Association,[3,4] the College of Physicians and Surgeons of Ontario,[5] the Canadian Medical Association,[6] the Information and Privacy Commissioner of Ontario[7] provide guidance about managing risks associated with privacy and social media but say little about the implications of mobile medical devices in delivering clinical care.

Privacy Commissioners do provide some guidance on what to do in event of a breach. For example, in Ontario, guidance from the Information and Privacy Commissioner calls for immediate implementation of a breach protocol; containment and evaluation of the scope of the breach; notification of the individuals affected; and subsequent investigation and remediation.[7] The Privacy Commissioner of Canada and the Information and Privacy Commissioners of British Columbia and Alberta released a joint document providing guidance on BYOD programs.[8] The document focuses on key

Key points

- The use of clinical photographs, taken with mobile devices, is changing health care for the better, but these images require special storage and consent.
- The breach of a provider's duty to ensure confidentiality of data stored on a mobile device can give rise to statutory and civil liability.
- The legal landscape continues to evolve as more common law and statutory causes of action are developed, exposing physicians to further risk.

Competing interests: Matthew Bromwich is the founder and Chief Medical Officer of Clearwater Clinical Ltd., a company that designs and manufactures mobile medical devices, mobile medical photography software and audiometry solutions. Rebecca Bromwich owns shares in Clearwater Clinical Ltd.

This article has been peer reviewed.

Correspondence to: Matthew Bromwich, MBromwich@cheo.on.ca

***CMAJ* 2016. DOI:10.1503/cmaj.160026**

privacy and security risks that should be considered when making decisions regarding such a program, including whether it is appropriate for an organization to implement one. They further provide a step-by-step methodology for the implementation of a BYOD program and specifically address pilot programs, training, security and management processes.

Health care providers and institutions risk civil liability if patient data stored on mobile devices are not handled securely. Legal suits are establishing new privacy torts (wrongful acts that result in injury to person, property or reputation and for which the injured party is entitled to compensation) related to privacy and autonomy.

For example, the tort of "intrusion on seclusion" is one mechanism of civil liability. The cause of a case in which unauthorized access to banking records gave rise to liability for intrusion on seclusion is now being applied to electronic medical records in two pending class action cases (*Hynes* v. *Western Regional Integrated Health Authority,* and *Hopkins* v. *Kay*), wherein scores of plaintiffs are seeking millions of dollars in compensation (Appendix 1). Hospitals, institutions and physicians risk liability. Further, in *Doe 464533* v. *N.D.*, civil liability for privacy breach was found where an intimate photograph intended for private viewing was publicly disclosed. In addition to intrusion upon seclusion, health care providers storing patient data on mobile devices may risk civil liability for breaches of confidence and privacy.

Further, statutory causes of action are being created to address privacy of electronic records and images. For instance, Manitoba has recently enacted legislation creating the tort of "nonconsensual distribution of intimate images." The province's Intimate Image Protection Act came into force in 2016. Although no other Canadian jurisdiction has similar legislation yet, such laws may be coming.

Mobile devices are revolutionizing the practice of medicine, but there are substantial risks in terms of data and image privacy. Legislation, the common law, regulations and policy guidance are striving to keep pace. It is incumbent upon health care providers together to study how mobile technologies are used and find ways to manage these resources to ensure that benefits are maximized and risks to patients' privacy and to physicians are mitigated.

References

1. *BYOD trends in healthcare: an industry snapshot*. Springfield (VA): SPOK; 2015. Available: http://20da214ed901ee90160e-913cb2fc6f14dcd4af57050fca98d3d4.r72.cf2.rackcdn.com/IB-AMER-BYOD-2015-Survey.pdf (accessed 2015 Oct. 2).
2. *Third annual benchmark study on patient privacy and data security*. Traverse City (MI): Ponemon Institute; 2015. Available: www2.idexpertscorp.com//resources/single/third-annual-benchmark-study-on-patient-privacy-data-security/r-general (accessed 2015 Oct. 2).
3. *Using electronic communications, protecting privacy: duties and responsibilities*. Ottawa: Canadian Medical Protective Association; 2013. Available: www.cmpa-acpm.ca/-/using-electronic-communications-protecting-privacy (revised 2016 Jan.; accessed 2015 Oct. 2).
4. *Protecting patient health information in electronic records: duties and responsibilities*. Ottawa: Canadian Medical Protective Association; 2013. Available: www.cmpa-acpm.ca/-/protecting-patient-health-information-in-electronic-records (accessed 2015 Oct. 2).
5. *Safe and effective office-based practices*. Toronto: College of Physicians and Surgeons of Ontario; 2012. Available: www.cpso.on.ca/Policies-Publications/CPGs-Other-Guidelines/Other-Guidelines/Safe-and-Effective-Office-Based-Practices (accessed 2015 Oct. 2).
6. *Guiding principles for physicians recommending mobile health applications to patients* [policy statement]. Ottawa: Canadian Medical Association; 2015. Available: https://www.cma.ca/Assets/assets-library/document/en/advocacy/cma_policy_guiding_principles_for_physicians_recommending_mobile_health_applications_to_patients_pd1-e.pdf (accessed 2016 Apr. 22).
7. Cavoukian A. *What to do when faced with a privacy breach: guidelines for the health sector*. Toronto: Information and Privacy Commissioner of Ontario; 2015. Available: www.ipc.on.ca/images/Resources/up-hprivbreach.pdf (accessed 2015 Oct. 2).
8. *Is a bring your own device (BYOD) program the right choice for your organization*? Office of the Privacy Commissioner of Canada/Office of the Information and Privacy Commissioner of British Columbia/Office of the Information and Privacy Commissioner of Alberta; 2015. Available: www.priv.gc.ca/information/pub/gd_byod_201508_e.asp (accessed 2015 Oct. 2).

Affiliations: Department of Otolaryngology – Head and Neck Surgery (M. Bromwich), Children's Hospital of Eastern Ontario; Department of Law (R. Bromwich), University of Ottawa; Department of Law and Legal Studies (R. Bromwich), Carleton University, Ottawa, Ont.

Contributors: Both authors contributed to the conception, design and analysis for the work, drafted and revised the manuscript critically for important intellectual content, approved the final version to be published and agreed to act as guarantors of the work.